REMARKS/ARGUMENTS

Claims 7, 9-12, 21, 23-26, 30, and 34-38 are pending. Claim 38 has been appended. Claim 7 has been amended to correct minor grammatical informalities. The claims have not been otherwise amended.

Claims 1, 2, 4-6, 13, 14, 16-20, 27-29, 34, and 36 are rejected under 35 U.S.C. § 102(a) as being anticipated by Schneier et al., U.S. Patent No. 5,956,404 ('404 patent).

Claims 7, 9-12, 21, 23-26, and 30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier et al., U.S. Patent No. 5,978,475 ('475 patent) in view of the '404 patent.

Claim 33 was inadvertently canceled in the response filed September 13, 2005. Accordingly, it is being resubmitted as appended claim 38.

The present invention sets forth a digital signature verifying method. The method comprises accepting a digital-signature-attached message. A log list of a digital signer is acquired. The originator of the digital-signature-attached message is authenticated if log data of the message is registered in the log list.

The '475 patent relates to the generation of a secure audit log. The basic idea of the audit log is to enable reconstructing an event that happened in the past. Col. 1, lines 5-7. This is a significant distinction from the present invention which, as recited in the pending claims, includes a log list that is used to authenticate the origin of a digital-signature-attached message as part of the process of receiving the digital-signature-attached message. Generating a secure audit log as disclosed in the '475 patent in and of itself does not suggest authenticating the originator of a message by looking at the audit log to determine if the log data of the message is registered therein. The '475 patent relates only to the generation of a secure audit log; the '475 patent does not disclose sending messages among machines and verifying the messages being sent using a log file.

The '475 patent discloses that an untrusted machine U creates an audit log. A trusted machine T receives the audit log and can validate the audit log. Col. 12, line 59 to col. 13, line 10. The '475 patent also discloses that a partially trusted machine V can verify or read some

portion of the audit log. See column 13, line 11 to column 14, line 20. The examiner cited the processing performed by V in support of the Section 103 rejection of remaining independent claims 7, 21, and 30.

Lines 15-16 at column 13 describe the partially trusted machine V receiving a message M1. This message is a response message that was created during a startup interaction between the machines U and T. Col. 10, lines 15-35. As will become apparent, the audit log is not checked to confirm the originator of message M1. The focus of the '475 patent is not on the response message M1, but rather on how an audit log that is generated by untrusted machine U can be validated by a trusted machine T and by a partially trusted machine V.

With respect to partially trusted machine V, A portion of the audit log is sent from T to V, namely, entries L0 to Lf (col. 13, lines 17 and 18) so that V can read data in some of those entries (Id at lines 18 and 19). The '475 patent then discloses steps "to verify the subset." Id at line 22. A review of the discussion at lines 23-33 reveals a description for verifying each entry in the subset that is received by V. Therefore, contrary to the examiner's assertion, the '475 patent does not disclose in lines 23-33 "checking whether log data of said digit-signature-attached message is registered in said log list." The '475 patent quite clearly states for step 610 that "V goes through the log entries L0 to Lf, verifying that each entry Yj in the hash chain is correct." Lines 23-24. A review of the steps 620 and 630 likewise does not reveal "checking whether log data of said digit-signature-attached message is registered in said log list." There is no discussion relating to validating the response message M1 by the use of entries in the audit log.

The '404 patent was cited in the Section 103 rejection of independent claims 7, 21, and 30 for showing accepting a message wherein the message may have been distributed by a digital signer to be verified. The '404 patent, however, does not disclose the specific aspects of the present invention as recited in the pending claims. In particular, the '404 patent does not disclose a log list, or authentication of an originator of a message by determining if log data of the message is registered in the log list.

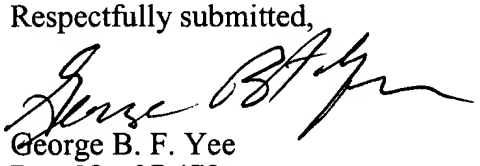
For at least any of the foregoing reasons, the '475 patent and the '404 patent considered separately or together, neither anticipate the present invention nor render obvious the present invention.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



George B. F. Yee
Reg. No. 37,478

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
GBFY:cmm
60431813 v1